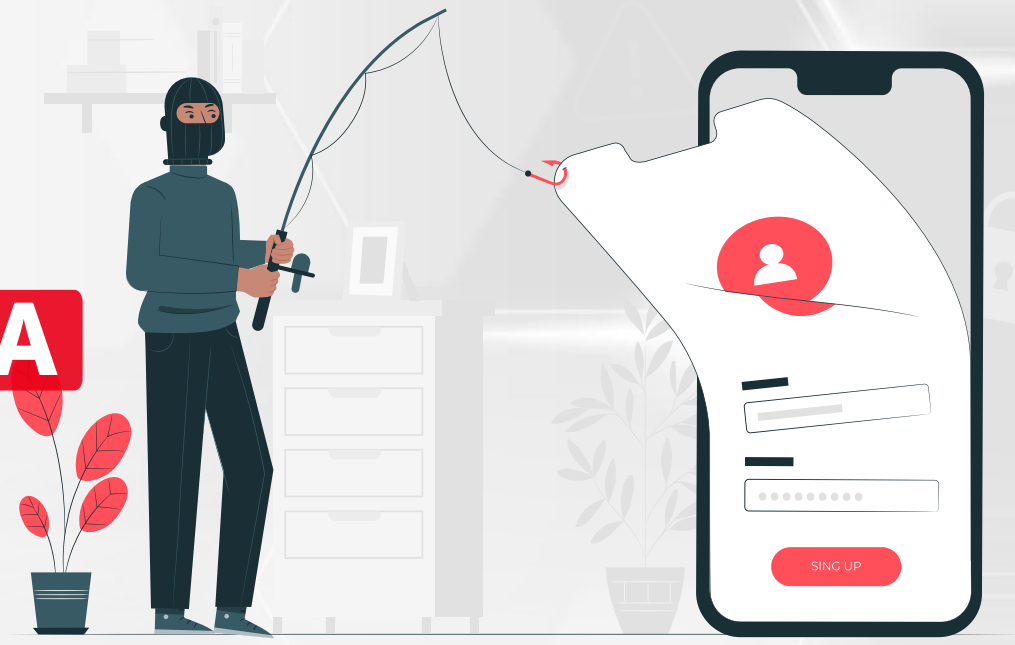
Noticias FONAFE

PHISHING: EL ANZUELO EN TU BANDEJA DE ENTRADA



Diariamente nos llegan varios correos a nuestra bandeja de entrada, una parte de ellos son publicidad no deseada y correos fraudulentos que nuestros gestores de correo filtran; sin embargo, algunos sí llegan a nuestra bandeja y es por ello la importancia de conocer cómo funciona el fraude electrónico conocido como PHISHING y, sobre todo, cómo debemos actuar para prevenirlo.

Esta práctica de manipulación es usada por los ciberdelincuentes para obtener información confidencial de los usuarios, haciéndose pasar por una fuente confiable, interna o externa, a la organización. La palabra proviene de fishing (pesca en inglés) pues es, justamente, mediante una carnada, que el estafador busca acceder de manera ilegal a dispositivos para suplantar identidades y robar credenciales, dinero y datos sensibles.

Los ciberdelincuentes solo necesitan unos minutos...

para poner el anzuelo, enganchar y atrapar a su víctima de PHISHING para luego aprovechar ese éxito en un ciberataque más amplio contra la organización. A continuación, un ejemplo:

Eligen a la víctima

un ciberdelincuente lanza una campaña de phishing a destinatarios de correo electrónico aleatorios de FONAFE (los correos fueron obtenidos de una violación de datos anterior).

Ponen el anzuelo

Lupita, colaboradora de FONAFE, abre el correo electrónico de phishing y ve un mensaje convincente sobre un documento que se va a descargar a través de un link. Es convincente porque el remitente parece ser su jefe con un correo falso.

Enganchan con el objetivo

Lupita está muy ocupada y, sin verificar previamente el correo, hace clic en el enlace malicioso que la lleva a un sitio web falso en donde le piden que ingrese sus credenciales de inicio de sesión de su computadora. Ella los ingresa y abre el documento que contiene malware oculto.

Realizan acciones maliciosas

Sin darse cuenta, el malware se descarga y luego se propaga rápidamente a través de la red de FONAFE, permitiendo al ciberdelincuente robar credenciales y datos confidenciales de la organización. En algún momento del ataque, las notas de rescate comienzan a aparecer en las pantallas de los colaboradores y las operaciones se detienen.

ACCIONES PREVENTIVAS

Las instituciones confiables **nunca solicitan datos mediante un e-mail.**

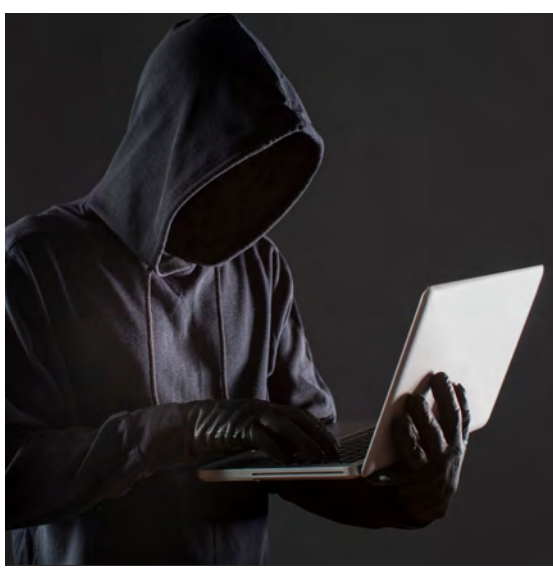
Si te llega un enlace sospechoso no lo abras, escribe en la barra de direcciones el nombre del sitio.

Si sospechas del correo verifica su autenticidad

Si te llega un correo electrónico dudoso **nunca hagas clic en los enlaces que contenga.**

Verifica tus cuentas periódicamente, evita fraudes.

Actualiza el sistema operativo constantemente, para eliminar debilidades.



ESTADÍSTICAS

Algunos reportes indican que el PHISHING es el ciberataque que más incrementó en Perú luego de la pandemia.

Fuente: MARSH

Según el estudio “Estado del Riesgo Cibernético en Latinoamérica en Tiempos del Covid-19”, un 49% de empresas peruanas encuestadas notó un aumento en los ataques cibernéticos entre el 2020 y el 2021, siendo la suplantación de identidad (phishing) el ciberataque más común.

El estudio se obtuvo de los resultados de una encuesta hecha a más de 600 empresas de la región, en 18 países y en más de 20 sectores.

Solo un 20% de las empresas encuestadas aumentó su presupuesto en ciberseguridad.